FM 74: Secure Communication & Computation III

Time: Thursday 14:00–15:30 Location: 1009

Invited Talk FM 74.1 Thu 14:00 1009

Quantum Computing and Cryptography — •Nico Döttling — CISPA Helmholtz Center for Information Security

In the early 1990s cryptography went into a foundational crisis when efficient quantum algorithms were discovered which could break almost all public key encryption schemes known at the time. Since then, an enormous research effort has been invested into basing public key cryptography, and secure computation in general, on problems which are conjectured to be hard even for quantum computers. This research program has been a tremendous success, resulting in cryptographic milestones such as fully homomorphic encryption, which was not known from pre-quantum assumptions. In this talk we will survey several recent developments in the field and provide a perspective on cryptographic protocols for quantum computations.

FM 74.2 Thu 14:30 1009

ppKTP Entangled Photon Source Study and a New Scheme — •Adrià Sansa Perna[1] and Fabian Steinlechner[2] — [1]Friedrich-Schiller University Jena, Abbe School of Photonics, Albert-Einstein-Str. 5, 07745 Jena, Germany. — [2]Fraunhofer Institute for Applied Optics and Precision Engineering IOF Albert-Einstein-Straße 7 07745 Jena, Germany.

An ultra-bright ppKTP crossed-crystal entangled photon source ready for use in quantum cryptography is designed and studied, leading to the possibility of a new entangled photon source scheme. First, a theoretical study of the efficiency parameters of the source is modelled taking into account deviations in the profile of the entangled photons. The source is thereafter build consistently with this results. It is shown to have a high brightness of 1.78 milion pairs/s/mW a brightness of the order of more complex interferometric sources, and a good quantum state fidelity of 95.6%. Its high brightness allows for the further study of the beam profile of the SPDC generated at different temperatures. This study of the beam profile allows the characterization of the SPDC emission in temperatures below phase-matching, and SPDC is seen to form a ring profile. The profile observed is modelled theoretically and the total amount of photons generated at different phase-matching conditions is calculated. This reveals the possibility of a new kind of source capable of delivering simultaneously entangled photons to various pairs of users. This new scheme for a source would allow to increase the number of users connected in a quantum network, one of the key aspects missing in developing quantum cryptographic technologies.

FM 74.3 Thu 14:45 1009

Quantum key distribution with a hand-held sender unit — Gwenaelle Vest[1], •Peter Freiwang[1], Jannik Luhn[1], Tobias Vogl[2], Markus Rau[1], Wenjamin Rosenfeld[1], and Harald Weinfurter[1,3] — [1]Ludwig Maximilian Universtity (LMU), Munich, Germany — [2]Australian National University (ANU), Canberra, Australia — [3]Max Planck Institute of Quantum Optics (MPQ), Garching, Germany

QKD enables secure communication by detecting eavesdropping attacks. While impressive progress was made in the field of long-distance implementations, user-oriented applications involving short-distance links have mostly remained overlooked. In this work we report on a hand-held free-space QKD system including a micro-optics based sender unit. This system implements a BB84-protocol employing polarization encoded faint laser pulses at a rate of 100 MHz. Unidirectional beam tracking and live reference-frame alignment systems at the receiver side enabled a stable operation over tens of seconds when holding the portable transmitter at a distance of 30 cm. Successful key exchange was performed by different untrained users with an average link efficiency of about 20 % relative to the case of the transmitter being stationary mounted and aligned with key rates ranging from 4.0 kbps to 15.3 kbps at an average QBER of 2.4 %. Given its compactness, this versatile sender unit is also well suited for integration into free-space communication systems for urban or even satellite applications.

FM 74.4 Thu 15:00 1009

Requirements for QKD ground station facilities — •Conrad Rössler[1,2], Kevin Günthner[1,2], Ömer Bayraktar[1,2], Jonas Pudelko[1,2], Kevin Jaksch[1,2], Imran Khan[1,2], Gerd Leuchs[1,2], and Christoph Marquardt[1,2] — [1]Max Planck Institute for the Science of Light, Staudtstraße 2, 91058 Erlangen, Germany — [2]Friedrich Alexander University Erlangen-Nuremberg, Staudtstraße 7/B2, 91058 Erlangen, Germany

During the last years, several space-based [1] quantum key distribution (QKD) setups were presented by various research groups and commercialization is about to start. We want to give insight into several requirements one needs to consider for the design of a space-based QKD system with a focus on the ground station. Both physical parameters as laser wavelength, aperture size, satellite orbit and the Doppler shift resulting from the satellites movement will be part of this presentation as well as a comparison of several encoding protocols. It will also be discussed if and how operation in urban environment is possible, since most research on space communication takes place in wisely chosen locations, usually with very low light pollution.

[1] I. Khan et al., Opt. Photonics News 29(2), 26-33 (2018)

FM 74.5 Thu 15:15 1009

Quantum Key Distribution with Small Satellites — •Ömer Bayraktar[4], Peter Freiwang[3], Daniel Garbe[1], Matthias Grünefeld[6], Roland Haber[1], Lukas Knips[5], Christoph Marquardt[4], Leonhard Mayr[3], Florian Moll[2], Jonas Pudelko[4], Benjamin Rödiger[2], Wenjamin Rosenfeld[3], Klaus Schilling[1], Christopher Schmidt[2], and Harald Weinfurter[1,5] — [1]Center for Telematics (ZfT), Würzburg, Germany — [2]German Aerospace Center (DLR) IKN, Oberpfaffenhofen, Germany — [3]Ludwig-Maximilian-University (LMU), Munich, Germany — [4]Max Planck Institute for the Science of Light (MPL), Erlangen, Germany — [5]Max Planck Institute of Quantum Optics (MPQ), Garching, Germany — [6]OHB System AG, Oberpfaffenhofen, Germany

QKD to satellites will be an important element enabling secure communication in future quantum safe network structures. After the first successful demonstration by the Chinese satellite MICIUS, the question arises how small a satellite can be designed. The space mission QUBE will test two highly integrated QKD sender modules and a quantum random number generator in a three unit CubeSat (10 x 10 x 30 cm^2). The optical communication terminal OSIRIS (effective aperture 20 mm) provides a link from a low earth orbit (LEO, 500 km) to the optical ground station (60 cm telescope) at the DLR in Oberpfaffenhofen. Quantum payloads and OSIRIS require approximately one unit in volume while the remaining two units needed for systems to operate the satellite.